



POLICE DEPARTMENT

-----X
In the Matter of the Disciplinary Proceedings :
- against - : FINAL
Police Officer Nicholas Amatulli : ORDER
Tax Registry No. 923502 : OF
Fleet Services Division : DISMISSAL
-----X

Police Officer Nicholas Amatulli, Tax Registry No. 923502, Shield No. 8370, Social Security No. ending in [REDACTED] having been served with written notice, has been tried on written Charges and Specifications numbered 2014-11147, as set forth on form P.D. 468-121, dated March 17, 2015, and after a review of the entire record, has been found Guilty as charged of Specification Nos. 1 & 2.

Now therefore, pursuant to the powers vested in me by Section 14-115 of the Administrative Code of the City of New York, I hereby DISMISS Police Officer Nicholas Amatulli from the Police Service of the City of New York.


WILLIAM J. BRATTON
POLICE COMMISSIONER

EFFECTIVE: 0001 Hrs. September 18, 2015



POLICE DEPARTMENT

August 31, 2015

-----X
In the Matter of the Charges and Specifications : Case No.
- against - : 2014-11147
Police Officer Nicholas Amatulli :
Tax Registry No. 923502 :
Fleet Services Division :
-----X

At: Police Headquarters
One Police Plaza
New York, New York 10038

Before: Honorable Robert W. Vinal
Assistant Deputy Commissioner Trials

APPEARANCE:

For the Department:

Daniel Maurer, Esq.
Department Advocate's Office
One Police Plaza
New York, New York 10038

For the Respondent:

John Tynan, Esq.
Worth, Longworth & London, LLP
111 John Street-Suite 640
New York, New York 10038

To:

HONORABLE WILLIAM J. BRATTON
POLICE COMMISSIONER
ONE POLICE PLAZA
NEW YORK, NEW YORK 10038

The above-named member of the Department appeared before me on December 30, 2014, January 28, 2015, March 17, 2015 and March 20, 2015¹ charged with the following:

1. On or about and between January 26, 2013 and March 31, 2013, Police Officer Nicholas Amatulli, currently assigned to Fleet Services Division, but while assigned to the 108 Precinct, accessed and downloaded to his personal computer and/or hard drive, videos, images, and/or photographs of pornography depicting sexual acts involving a child and/or children less than sixteen years of age.

P.G. 203-10, Page 1, Paragraph 5 – PROHIBITED CONDUCT
CONDUCT - GENERAL REGULATIONS

2. Police Officer Nicholas Amatulli, currently assigned to Fleet Services Division, but while assigned to the 108 Precinct, on or about May 2, 2013, was in possession of electronic files created on two occasions, October 29, 2007 and January 12, 2008, which contained videos, images and/or photographs of pornography depicting sexual acts involving a child and/or children less than sixteen years of age. (*As amended*).

N.Y.S. Penal Law 263.11 – POSSESSING AN OBSCENE SEXUAL
PERFORMANCE BY A CHILD

N.Y.S. Penal Law 263.16 – POSSESSING A SEXUAL PERFORMANCE
BY A CHILD

The Department Advocate's Office was represented by Daniel Maurer, Esq.
Department Advocate's Office, and Respondent was represented by John P. Tynan, Esq.
A stenographic transcript of the trial record has been prepared and is available for the
Police Commissioner's review.

DECISION

Respondent is found Guilty of Specification Nos. 1 and 2.

¹ The trial record was held open until April 30, 2015, for the submission of written closing arguments by the parties.

SUMMARY OF EVIDENCE PRESENTED

The Department Advocate called three witnesses: Detective Damon Gergar, Sergeant Jorge Gomez and Sergeant Juan Bastidas. Respondent testified on his own behalf.

Detective Gergar, who is assigned to the Vice Major Case Unit, testified that he has investigated numerous child pornography cases since 2009. (Tr. 12). On March 26, 2013, he was reviewing various databases in an attempt to locate subjects in the New York City area who were downloading and sharing child pornography. (Tr. 13-14). His search revealed a Verizon Internet Protocol (IP) address (which is a unique set of numbers given out by an Internet service provider to every person who has an account) located in [REDACTED] that had shared and downloaded 148 files containing possible child pornography beginning in January 2013. (Tr. 14). Gergar obtained, via a subpoena, the subscriber information associated with this Verizon IP address, (Tr. 15) which was connected to a Verizon FIOS account registered to Respondent. (Tr. 16). The Internal Affairs Bureau ("IAB") examined Respondent's time and leave history and determined that all of the 148 downloads in question occurred when Respondent was off duty or on vacation. (Tr. 141-42).

IAB executed search warrants at Respondent's residence in [REDACTED] on May 2, 2013. When IAB investigators arrived at the front door of Respondent's residence, Respondent's father, who lives on the second floor of the two-family home, allowed the investigators entry. (Tr. 143). Respondent was located in the basement with the basement door locked. (Tr. 143-44, 313-14). Gergar recalled that during execution of a search warrant, he observed a monitor turned on in the basement and plugs "all over the

place” but no tower computer attached. (Tr. 46). He testified that he asked Respondent where the tower computer was and Respondent told him he did not have a tower computer. Gergar recalled that the desktop tower computer was later found “hidden” in the basement “behind a bunch of junk.” (Tr. 44-45). He did not ask Respondent why it was hidden. (Tr. 50).

Forensic analysis of this computer revealed that an external Western Digital hard drive and a HP thumb drive were plugged into Respondent’s desktop computer on April 28, 2013 at approximately the last time the IP address was seen sharing child pornography. (Tr. 47-48, 274-75). The Department was not able to find and retrieve those devices during its search. (*Id.*). Two laptops, one desktop computer and two external hard drives were confiscated for analysis. (Department’s Exhibit (“DX”) 1).

Gergar testified that he personally viewed some of the 148 files shared on Respondent’s IP address. Gergar provided a sampling of the files to IAB investigators and described their contents in detail before this tribunal. (Tr. 216). The names and contents of these sample files, as described by Gergar, are listed below:

- #59- “**[REDACTED]** center”- video of an 8 year-old girl masturbating, performing fellatio and having sexual intercourse with an adult male
- #69- “*Thai [REDACTED] 2009 Lollipop*”- video of young teen girl (approx. 12-14 yrs.) rubbing the breasts and genitals of a young girl (approx. 5-7 yrs.)
- #84- “**[REDACTED]**(**[REDACTED]**)(**[REDACTED]**)(*India Lolita*)”- video of a preteen girl (approx 10-12 yrs.) holding the penis of an adult male, performing oral sex on him and having vaginal intercourse with him and video of other young girls performing sex acts
- #86- “**[REDACTED]** pedo”- video of preteen girl and boy showing them fondling each other’s genitals and close-ups of their genitals. Various other clips of children posing and a young boy and girl having intercourse.
- #87- “*Euman 11 yo 12 yo [REDACTED] Favorite Bambina Collection- Real Child Porn Illegal Preteen Underage Lolita Kiddy Incest Little Girl Rape Anal Cum*”

² **[REDACTED]** was defined by Gergar as a “common term used by pedophiles to search for child pornography on the Internet.” Gergar explained that it stands for “**[REDACTED]**.” (Tr. 19).

Sex"- video of naked prepubescent female (approx. 9-12 yrs.) spreading her genitalia, posing, masturbating, masturbating an adult male and then having vaginal intercourse with the adult male.

- #100- "8.mpg"- video of under-14 female performing oral sex on an adult male, masturbating the male and being anally penetrated by his penis
- #134- "115.mpeg"- video showing close-up shots of a preteen girl's nude genital area
(DX 2 (highlighted selections); Tr. 239-54).

While database detector programs showed these files being shared over Respondent's IP address from [REDACTED] these files were not found on Respondent's computers or other electronic equipment that was retrieved and analyzed by IAB investigators. (Tr. 258-60). However, an external hard drive that was never recovered was determined to have been plugged into Respondent's computer at one point when these files were being shared. (Tr. 47-48, 274-75).

Other videos and files, however, were found on another Western Digital external hard drive retrieved from Respondent's residence. (Tr. 81). Forensic analysis revealed that said hard drive contained a "Hidden" folder that would not ordinarily be visible unless the user typed in a specific command. (Tr. 82; DX 1 at p.6). A forensic search for child pornography showed four possible child pornography video files that were downloaded, accessed and subsequently deleted from the hidden folder of this hard drive. (Id.). The titles of these deleted files are:

- "([REDACTED] 022 Asian [REDACTED] (tied 8 yo Cambodian boom-boom girl fucked + raped by sex tourist [REDACTED] - file created 11/07/2007; last accessed 11/07/2007
- "([REDACTED] ([REDACTED] St. Petersburg 7 yo girl in Uncle's bed. Excellent Oral. [REDACTED] Childlover"- file created 11/07/2007; last accessed 11/07/2007
- "([REDACTED] Russian girl 13 yo New"- file created 10/29/2007; last accessed 11/23/2007
- "([REDACTED]) Incest (11) Mom lets 13 yo Son Fuck Her"- file created 10/29/2007; last accessed 11/06/2007

These files were not viewable by investigators because they had been deleted. (Tr. 198-99). Although they were downloaded to Respondent's hard drive, it could not conclusively be determined whether they were viewed by Respondent.

The search on the external hard drive also revealed several files that had not been deleted, including Respondent's family and military photos. All the photo and video hash values were compared against the Access Data Known File Filter database of known child pornography. The results revealed eight possible child pornography videos and one photo on the hard drive. (DX 1 at p.7). Those files were viewed by Sergeant Gomez of the IAB Computer Crimes Unit and Detective Gergar of the Vice unit. Gergar, drawing on his years of experience dealing with child pornography cases, described the content of the files as follows. His statements as to the ages of the subjects of the videos and the acts depicted in the videos were not challenged by Respondent's counsel. (Tr. 225-26, 285).

- "345678.MPG"- video of 15 year-old girl engaged in oral sex. *File created 10/29/2007; last accessed 01/19/2012.*
- "54+6.mpg"- video of 14 year-old boy receiving oral sex. *File created - 10/29/2007; last accessed 09/15/2011.*
- "_ASHA.AVI"- video of 12-13 year-old girl nude and dancing. *File created - 10/29/2007; last accessed 03/25/2010.*
- "WEWTR.MPG"- video of 12 year-old girl performing oral sex on a male and subsequently having intercourse. *File created -10/29/2007; last accessed 09/11/2009.*
- "RUSSIANS.AVI"- video of 13-14 year-old girl engaged in sex acts. *File created 01/12/2008; last accessed 07/23/2009.*

Three other videos and one photo were deemed "age difficult,"³ as Gergar could not determine with certainty if the subject was underage. (Tr. 214-15).

³ Because these videos and photo could not be conclusively deemed child pornography due to the difficulty in determining the subjects' ages, Specification 2 was amended, on the record, to delete the dates of November 7, 2007 and July 3, 2008 and change the original wording of "on four occasions" to "on two occasions." (Tr. 230-31).

There was no child pornography or peer to peer software, which is the more common means of downloading child pornography, found on a Toshiba laptop recovered from the second floor of the residence. (DX 1 at p.1). Respondents' parents live on the second floor of the two-family residence. (Tr. 296). Another Toshiba laptop, recovered from the first floor where Respondent resided with his wife and two small children, also showed no child pornography. (DX 1 at pp.1-2). Forensic analysis did reveal, however, that an unknown user unsuccessfully attempted to use this laptop to download movies, including a file entitled "skinnyteens286," via the eMule peer-to-peer software directed to a WD Passport hard drive. The search further revealed that an attempt was made using this laptop to download the eMule peer-to-peer software shortcut to a WD Passport hard drive connected to the computer on April 18, 2013. (Id.).

Additionally, a search for files containing the term "[REDACTED] ([REDACTED])" revealed that an unsuccessful attempt was made to download a video entitled "11yo CrystalMbate" to the laptop. Because the download was unsuccessful and the file was recovered from unallocated space, the time and date of when the download attempt was made could not be determined. (DX 1 at p.2).

An Internet search history showed thirteen visits to the website [www.\[REDACTED\].com](http://www.[REDACTED].com) in April 2013. (Id.). Respondent admitted he had been visiting this site to access adult pornography since learning about it from a friend. (Tr. 311).

A search of Respondent's desktop tower computer, which was located in the basement, revealed that the eMule peer-to-peer file sharing software was loaded on the desktop in April 2010 and last accessed on March 8, 2012. (DX 1 at p.2). The search

further showed that attempts were made to download movie files directed to a WD Passport hard drive but the contents of those files and the dates and times of the attempts for all but one file could not be determined. (DX 1 at pp. 3-4).

All of the computers were examined to determine if they were accessed when any of the files in question were downloaded from the peer-to-peer applications. None of the computers were accessed during the dates and times that the files in question were downloaded. (DX 1 at p.7).

He explained that prior to the execution of the search warrant, he conducted a "wireless survey" of Respondent's residence where he went to the residence and stood outside to see if he could locate open WiFi signals. (Tr. 42). Gergar did not observe any open wireless WiFi connections near Respondent's home and thus determined that only those with a password could access Respondent's WiFi network. He noted that in his years of experience working with law enforcement across the country on child pornography cases, he has never heard of a hacker putting child pornography on someone else's computer. (Tr. 51).

Gergar testified that he found only adult pornography on Respondent's computers and that Respondent admitted to him that he visited [REDACTED].com. (Tr. 49-50). Gergar characterized the website "[REDACTED].com" as "on the cusp" of pornography and child pornography and catering to people that "want to look at younger girls." (Tr. 22).

He further explained that one must search for child pornography using specific keywords, therefore making it impossible to download it accidentally even when searching for adult pornography. (Tr. 51-53). Peer-to-peer sharing software is the more common way of accessing child pornography, according to Gergar, because it allows files

to be obtained much more quickly. (Tr. 19-20, 262-64). He noted that the most common search term is "[REDACTED]" which stands for "[REDACTED]." (Tr. 209-210).

Gergar was not able to view the four deleted videos found on Respondent's hard drive but testified that the names of the files stood out to him as well known within the pedophile/child pornography community. (Tr. 208-09). He explained that in addition to "[REDACTED]" which was in three of the four titles, "[REDACTED]" is one of the most popular child pornography series on the Internet. (Tr. 209-210). He noted that "[REDACTED]" and "[REDACTED]" are popular child pornography series as well as "[REDACTED]" and "[REDACTED]," all of which were contained in the deleted file names. (Tr. 210-12).

Gergar explained that it is possible for someone not to be physically in their residence but still downloading and/or accessing child pornography. This can be done by having programs that give remote access to your home computer or simply by leaving the computer on with the peer-to-peer software running ongoing searches. (Tr. 257-58).

On cross examination, Gergar admitted that no remote access accounts were found on any of Respondent's electronic equipment. (Tr. 260). He acquiesced that it is not possible to determine with certainty who received or accessed the child pornography files that were being shared over Respondent's IP address. (Tr. 265). He further testified that there is no way to determine with certainty who downloaded the child pornography videos that were found on Respondent's external hard drive. (Tr. 268-69). Gergar agreed that eMule peer-to-peer software can be used to download not only child pornography but music, movies and adult pornography. (Tr. 280).

Sergeant Gomez, who is assigned to IAB's Computer Crimes Unit, generated a forensic report following the seizure of Respondent's computers and electronic devices. (Tr. 76-78). The contents of that report (DX 1) are described above.

On cross examination, Gomez agreed that the eMule is just one of a number of legally available peer-to-peer software programs and that large files can be downloaded much more quickly with peer-to-peer software. (Tr. 91-93). He acknowledged that pornography can also be downloaded directly from the Internet and that Respondent's external hard drive had adult pornography downloaded onto it. (Tr. 95). He further agreed that [REDACTED] is a legally accessible pornography website. (Tr. 95, 106).

He testified that he did not know how long Respondent had been in possession of his computer and did not know whether he bought it and the hard drive new or used. (Tr. 103-04). He agreed that there was no definitive indication that Respondent was the individual who created or last accessed the four child pornography titles that were found on his Western Digital external hard drive. (Tr. 115-16).

Gomez stated that he searched all the computers based on the times and dates that Gergar had observed child pornography traffic being shared over Respondent's IP address and determined that the computers showed no peer-to-peer activity at those times. (Tr. 122). He acquiesced that nothing in his forensic investigation clearly determined that Respondent had been actively downloading or possessing child pornography. (Tr. 124-25).

On redirect, Gomez explained that child pornography must be specifically sought out by typing in search terms. (Tr. 125-26). He further clarified that an individual need

not be sitting behind their computer to share a child pornography file if the computer is on and the peer-to-peer software is running. (Tr. 127-28).

He also testified that all of Respondent's family and military photos, recovered from his Western Digital hard drive, were copied onto the hard drive on August 5, 2007.⁴

Sergeant Bastidas, who is assigned to IAB, became involved after being advised by [REDACTED] Vice that they had intercepted child pornography downloads to Respondent's IP address. (Tr. 137-38). He stated that a subsequent investigation revealed that on all the download dates in question, Respondent was on leave or a regular day off. (Tr. 141-42). He testified that a review of Respondent's personnel file revealed that Respondent was an electronics (avionics) specialist in the military. (Tr. 149).

Bastidas recalled that he was present for the execution of the search warrants. When he entered the residence, he found that Respondent had locked himself in the basement. (Tr. 144). When he asked Respondent why he did not open the door, Respondent told him that he was filing comic books. Respondent also told him that his Internet connection was password-protected and that only he, his wife and his parents had access to the computers. (Tr. 146-48). Bastidas spoke with Respondent's father who asserted that he had never downloaded child pornography. (Tr. 148).

On cross-examination, Bastidas stated that he was not aware if Respondent was on military duty in Newburgh, New York on two of the dates his IP address was flagged by the Vice unit for child pornography. (Tr. 150). He further testified that he was unaware as to whether Respondent was in New Jersey on vacation from March 26 to

⁴ During redirect, the Department Advocate emphasized that child pornography videos were subsequently saved to the hard drive on October 29, 2007 and January 12, 2008, after the family photos were downloaded on August 5, 2007. (Tr. 187; see DX 1 at p.7).

March 30, 2013. (Tr. 157-58). [REDACTED] Assistant District Attorney Gasper informed him that the District Attorney was declining to prosecute Respondent because the storage device used to download the child pornography was not recovered during the searches at Respondent's residence. (Tr. 161).

On redirect examination, Bastidas testified that during Respondent's GO-15 on March 4, 2014, Respondent never mentioned that he was on military duty at any point during the dates in question. (Tr. 167-69).

Respondent denied that he had ever attempted to download child pornography or attempted to possess and/or store child pornography. (Tr. 318-19). He testified that he was assigned a scheduled military drill on February 9, 2013 and traveled to Newburgh, New York the night before. (Tr. 297). He recalled that he was notified that night that the drill was canceled due to inclement weather but opted to stay overnight in the barracks. (Tr. 298). Although not required, he stayed for the entire duration of the drill and returned to [REDACTED] in the late afternoon on February 10, 2013. He could not recall the exact time he departed the base. (Tr. 322). He explained that he has access to electronic equipment through his assignment in the Avionics Unit but did not bring his personal laptop because he "didn't need it," as there was no Internet service in the barracks. (Tr. 299-301). He denied remotely accessing his computers in [REDACTED] from Newburgh and denied attempting to download child pornography. (Tr. 301).

Respondent noted that he worked in the Summons Unit of the 108 Precinct beginning at 0500 hours the following day, February 11, 2013, but took lost time at approximately 1130 hours when he got a call that his son was sick and needed to be

picked up from school. (Tr. 302). He stated that he left work, went home and changed, got his son at school and arrived at the doctor's office in [REDACTED] at 1229 hours. He was unable to recall exactly what time he arrived home after the doctor's office. (Tr. 324). He denied using his laptop at any point that afternoon to access child pornography, asserting that he "didn't have time." (Tr. 304). He further denied ever attempting to access child pornographic websites or forums between January 26, 2013 and February 9, 2013 "through either of the computers...at [his] home." (Tr. 305).

Respondent next testified that he drove to New Jersey for a vacation with his wife and children on March 25, 2013. He stayed one night at the Coco Keys Water Park hotel, one night at his uncle's home in Egg Harbor and one night in Atlantic City at Caesar's. (Tr. 305-08). Respondent asserted he did not bring his laptop on vacation and was not remotely accessing his home computer. (Tr. 306-07). He noted, however, that his computers were "always" left on at his home. (Tr. 308). The family returned home from their vacation on the evening of March 28. Respondent denied downloading or viewing any child pornography between the evening of March 28 and April 1, 2013.

Respondent explained that he knew about peer-to-peer software and had the eMule software system downloaded on one of his computers. (Tr. 309-10). He stated that he used it to download music and "possibly" adult pornography.

On cross examination, he recalled using eMule to request and view pornography. (Tr. 333-34). He noted that he generally saved adult pornography to an external hard drive, which he also used for saving family and military photos, and further stated that he loaned out his external hard drive to other Marines because they exchange things on "a

lot of occasions.” (Tr. 312). He denied ever hearing or using the search term “ [REDACTED] ([REDACTED]) until this trial. (Tr. 311).

FINDINGS AND ANALYSIS

It is charged that Respondent accessed and downloaded to his personal computer and/or hard drive, videos, images, and/or photographs of pornography depicting sexual acts involving a child and/or children less than sixteen years of age, and that he was in possession of electronic files created on two occasions, October 29, 2007 and January 12, 2008, which contained videos, images and/or photographs of pornography depicting sexual acts involving a child and/or children less than sixteen years of age.

The Department presented strong circumstantial evidence at this trial that Respondent personally accessed and downloaded to an external hard drive pornography depicting sexual acts involving children less than sixteen years of age and that after he had deleted these files he placed this hard drive in his basement to avoid discovery by the Department of the fact that he had accessed and downloaded child pornography.

The Connection between Respondent's IP Address and Child Pornography Databases

Gergar offered unrefuted testimony that he has investigated numerous child pornography cases during the past six years for the Vice Major Case Unit and is very familiar with the databases that are used to locate individuals who are seeking to download and/or share child pornography.

On March 26, 2013, as he was reviewing these databases attempting to ascertain who the subjects were, he discovered a Verizon IP address located in [REDACTED] that had accessed 148 files containing possible child pornography beginning in January 2013.

Gergar obtained the subscriber information associated with this Verizon IP address and learned that it was connected to a Verizon FIOS account registered to Respondent. Gergar offered unrefuted testimony that a Verizon IP address is a unique set of numbers which is only provided by Verizon, as an Internet service provider, to the person who is the owner of the Verizon account. Gergar also offered unrefuted testimony that Respondent's Verizon IP address could be used only by entering a confidential password.

In his testimony at this trial, Respondent acknowledged that he had used his Verizon IP address to visit the website [REDACTED] and also used eMule, although he asserted that in doing so he was not attempting to access or download child pornography.

Gergar's unrefuted testimony combined with Respondent's acknowledgment that he used his Verizon IP password to visit the website [REDACTED] and also used eMule, establishes that it is more likely than not that it was Respondent who entered his personal password for his Verizon IP address to access 148 files containing possible child pornography.

The Results of the Search Warrants Executed at Respondent's Residence on May 2, 2013

The first search warrant that was executed at Respondent's residence on May 2, 2013, authorized only a search of the first floor of the residence. This search warrant resulted in the seizure of a laptop computer which contained no child pornography.

The second search warrant that was executed at Respondent's residence on May 2, 2013, authorized a search of the residence's basement. I credit Gregar's unrefuted testimony that an external computer hard drive was discovered in Respondent's basement.

Forensic Examination of the Hard Drive Discovered in Respondent's Basement

I credit Gomez's unrefuted testimony that he was able to recover a number of files which had been deleted on this external hard drive. As he detailed in his Forensic Report (DX 1 p. 6), four of these deleted files were videos and three of the file names for these videos contained the acronym "[REDACTED]" which Gregar testified is an acronym for "Pre-Teen Hard Core" and is used to designate that the video contains child pornographic content. The videos' names also variously contained the terms "[REDACTED]" "[REDACTED]" "[REDACTED]" and "[REDACTED]" which Gregar testified are well known search terms for seeking out child pornography or series depicting child pornography. The videos' names also variously contained the phrases: "tied 8 yo Cambodian boom-boom girl fucked + raped by sex tourist;" "7 yo girl in Uncle's bed. Excellent Oral;" "Russian girl 13 yo New;" and "Incest (11) Mom lets 13 yo Son Fuck Her."

Most significantly, as detailed at the end of his Forensic Report (DX 1 p. 7), Gomez was able to recover eight undeleted videos and one photograph. Gregar testified that he personally viewed these videos. Since he has been required to view numerous such videos, I credit Gregar's claim that he has developed expertise in accurately estimating the ages of the boys and girls seen in such videos. Therefore, I credit his estimation of the ages of the children seen in these videos. Gregar testified that "345678.MPG" is a video of a 15 year-old girl engaged in oral sex; "54+6.mpg" is a

video of a 14 year-old boy receiving oral sex; "ASHA.AVI" is a video of a 12-13 year-old girl nude and dancing; "WEWTR.MPG" is a video of a 12 year-old girl performing oral sex on a male and subsequently having intercourse; and "RUSSIANS.AVI" is a video of a 13-14 year-old girl engaged in sex acts.

Respondent's Behavior During the Execution of the Search Warrant

Respondent claimed that he has never accessed and downloaded to any personal computer hard drive videos or photos depicting sexual acts involving children less than sixteen years of age; and that he did not know that any such deleted videos or photographs were contained on the hard drive that was discovered in his basement. Respondent's claims are belied by his behavior and the statements he made during the execution of the search warrant. I credit the testimony of Bastidas, who was not shown to have any motive to want to cause trouble for Respondent, that when he entered the residence to execute the search warrant, he discovered that Respondent had locked himself in the basement and that when he asked Respondent why he did not open the door, Respondent told him that he was filing comic books. Gergar recalled that during the search of the basement, he observed a monitor turned on in the basement and plugs "all over the place" but no tower computer attached. When he asked Respondent where the tower computer was, Respondent told him he did not have a tower computer, even though a tower computer was later found "hidden" in the basement "behind a bunch of junk."

Respondent's behavior during the execution of the first search warrant supports a finding that it is more likely than not that he was the person who attempted to secrete the

tower in his basement behind "junk." Thus, I find that Respondent's behavior during the execution of the search warrant demonstrates a consciousness of guilt.

Respondent's Opportunity to Access Child Pornography via a Personal Computer

I credit the testimony of Bastidas that he compared the dates that child pornography downloads occurred with Respondent's time and leave records and determined that on all of the dates that downloads occurred, Respondent was either on leave or taking a regular day off. I find that it reflects more than mere coincidence that on all of the dates that downloads occurred, Respondent was not on duty but was available to use his personal computer because he was either on leave or taking a regular day off.

Respondent's Testimonial Demeanor at this Trial

Based on the nature of the accusations contained in these charges, a member of the service who is asserting that he has never engaged in the activity Respondent is charged with engaging in here would be expected to vociferously assert his innocence. However, during his testimony at this trial, when Respondent was asked whether he had ever downloaded and watched child pornography, he did not display revulsion or anger that such an accusation had been made against him. Rather he merely answered "no" in a quiet, emotionless, deadpan voice with a flat affect. That he is capable of voicing emotional indignation was demonstrated when he testified that in his opinion the officers who had executed the search warrants at his home had conducted themselves in an unprofessional manner. Since he failed to display similar indignation, or any other

emotion, when he was directly confronted with the accusation that he had downloaded and watched child pornography, his denial was unconvincing.

Respondent's Claims that Someone Else Must Have Accessed the Child Pornography

Bastidas testified that Respondent told him that his internet connection was password-protected and that only he, his wife and his parents had access to the personal computer in the residence. Respondent's father told Bastidas that he had never downloaded any child pornography and it is unlikely that Respondent's wife or his mother did so.

Also, the record is devoid of any evidence that someone had hacked Respondent's computer. Gregar confirmed Respondent's WiFi network was protected by a password. Respondent offered an unsupported assertion that the hard drive discovered in his basement apparently was purchased used and that the child pornography on it seemingly predates Respondent's possession. I reject this assertion because Gomez testified that all of the pertinent undeleted child pornography discovered on the external hard drive was saved to the hard drive on either October 29, 2007 or January 12, 2008. Since Respondent downloaded personal family and military photographs to this hard drive on August 5, 2007, it is clear that Respondent possessed the hard drive prior to the point in time when child pornography was saved to this hard drive. Moreover, the five undeleted child pornography videos contained on the hard drive were last accessed on January 19, 2012, September 15, 2011, March 25, 2010, September 11, 2009, and July 23, 2009. (DX 1, p. 7).

Respondent asserted that he could not have been home downloading child pornography on certain dates because he was in Newburgh, New York, attending a military exercise that was cancelled due to weather; taking his child to the doctor; and on vacation in New Jersey. Although Respondent offered documents (RX A-C) to support his claims that he was not at home, Gergar testified that Respondent did not have to be in physical proximity to his home computer to access child pornography. He could just leave his computer on with peer-to-peer software running in the background and an active search request pending or in progress. In this regard I find it significant that Respondent testified that his computer is "always on."

Finally, I reject his unsupported, self-serving testimony that he had loaned out his external hard drive to fellow Marines because they exchange things on "a lot of occasions" and one or more of these Marines must have accessed the child pornography discovered on the hard drive.

Respondent is found Guilty of Specification Nos. 1 and 2.

PENALTY

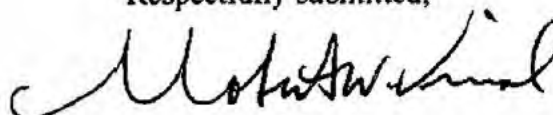
In order to determine an appropriate penalty, Respondent's service record was examined. See *Matter of Pell v. Board of Education*, 34 NY 2d 222 (1974). Respondent was appointed to the Department on July 7, 1999. Information from his personnel record that was considered in making this penalty recommendation is contained in the attached confidential memorandum.

Respondent has been found Guilty of having accessed and downloaded to his personal computer and/or hard drive, videos, images, and/or photographs of pornography

depicting sexual acts involving children less than sixteen years of age, and being in possession of electronic files created on two occasions which contained videos, images and/or photographs of pornography depicting sexual acts involving children less than sixteen years of age.

Accordingly, it is recommended that Respondent be DISMISSED from the New York City Police Department.

Respectfully submitted,



Robert W. Vinal
Assistant Deputy Commissioner – Trials

APPROVED

SER 1 8 2015

WILLIAM J. BRATTON
POLICE COMMISSIONER

POLICE DEPARTMENT
CITY OF NEW YORK

From: Assistant Deputy Commissioner - Trials

To: Police Commissioner

Subject: CONFIDENTIAL MEMORANDUM

POLICE OFFICER NICHOLAS AMATULLI
TAX REGISTRY NO. 923502
DISCIPLINARY CASE NO. 2014-11147

Respondent received an overall rating of 4.0 on his 2014 annual performance evaluation and 3.5 on his 2013 annual evaluation and 4.5 on his 2012 annual evaluation. He has been awarded four Meritorious Police Duty medals and three Excellent Police Duty medals. [REDACTED]

[REDACTED] He has no prior formal disciplinary record and no monitoring records.

For your consideration.



Robert W. Vinal
Assistant Deputy Commissioner – Trials